MIDTERM 1 MATH 103A Winter 2019
SOLUTIONS

1. Find integers s and t such that $1 = 5s + 13t$. Show that s and t are not unique.

One solution would be $t = 2$ and $s = -5$, which can be easily checked. For any solution s and t, we also get the solution $s + 13$ and $t - 5$. Indeed we would get

$$5(s + 13) + 13(t - 5) = 5s + 5 \cdot 13 + 13t + 13 \cdot (-25) = 5s + 13t + 65 - 65 = 1.$$

2. Calculate 2^{1207} mod 15. Justify your answer.

We have $2^4 = 16 = 1$ mod 15. We have $1207 = 4 \cdot 301 + 3$. Hence

$$2^{1207} = (2^4)^{301} 2^3 = 1^{301} 8 = 8 \text{ mod} 15.$$

3. Consider the group $\mathbb{Z}_{24}$.
(a) Find all the generators of $\mathbb{Z}_{24}$.

An element j in $\mathbb{Z}_{24}$ is a generator if and only if its order is 24. It was shown in class that the order of j is $24/gcd(j, 24)$. Hence we have to determine all j for which $gcd(j, 24) = 1$. These are

$$\{1, 5, 7, 11, 13, 17, 19, 23\}.$$

(a) Find all elements of order 6 in $\mathbb{Z}_{24}$.

By the same argument as before, we now have to find all j for which $gcd(j, 24) = 24/6 = 4$. These are

$$\{4, 20\}$$

(As 4 must divide j, it suffices to check the numbers 4, 8, 12, 16, 20.)

4. Find all subgroups of $U(9)$. Give a reason why the subgroups you have found are all there are.

We have $2^2 = 4$, $2^3 = 8$, $2^4 = 16 = 7$ mod 9, $2^5 = 2 \cdot 7 = 5$ mod 9 and $2^6 = 2 \cdot 5 = 10 = 1$ mod 9. Hence $\langle 2 \rangle = \{1, 2, 4, 5, 7, 8\}$. These are all elements of $U(9)$ (because $gcd(3, 9) = 3 = gcd(6, 9)$ and $gcd(0, 9) = 9$.) This shows that $U(9)$ is cyclic.

By a theorem in class, there exists exactly one subgroup for each divisor d of $|U(9)| = 6$. It is generated by 2^d. For $d = 1$ and $d = 6$ we get the subgroups $U(9)$ and $\{1\}$. For $d = 2$, we get the subgroup $\{4, 7, 1\}$ and for $d = 3$ we get $\{8, 1\}$.

5. Let G be a cyclic group of order 18, and let a be a generator of G. What is the order of $\langle a^{15} \rangle \cap \langle a^{10} \rangle$? Justify your answer!

We caclulate $gcd(15, 18) = 3$ and $gcd(10, 18) = 2$. Hence

$$\langle a^{15} \rangle = \langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18} = e\},$$

$$\langle a^{10} \rangle = \langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}, a^{16}, a^{18} = e\},$$

Hence the intersection of these two subgroups is given by $\{a^6, a^{12}, a^{18} = e\}$, i.e. it has order 3.